PTO 07-3736

French Patent

Document No. 2822255

METHOD FOR AUTOMATED AND SECURE ACCESS TO INTERNET PAGES, EMAIL MESSAGES, OR BANK ACCOUNTS

[Procédé d'accès automatisé et sécurisé à des pages Internet, des courriers électroniques, ou comptes bancaires]

Marguerite Paolucci et al.

UNITED STATES PATENT AND TRADEMARK OFFICE

Washington, D.C. April 2007

Translated by: Schreiber Translations, Inc.

Country	:	France
Document No.	:	2822255
Document Type	:	Patent
Language	:	French
Inventor	:	Marguerite Paolucci et al.
Applicant	:	Marguerite Paolucci et al.
IPC	:	G 06 F 9/445
Application Date	:	02/12/01
Publication Date	:	09/20/02
Foreign Language Title	:	Procédé d'accès automatisé et sécurisé à des pages Internet, des courriers électroniques, ou comptes bancaires
English Title	:	Method for Automated and Secure Access to Internet Pages, Email Messages, or Bank Accounts

/1[1]

The present invention relates to a method for automated access and/or connection and secured entry to the Internet that is compatible with all types of PCs using Windows 95, 98, 2000 or NT operating systems that have a simple drawer-type CD reader, for private or even public use, such as in cyber cafés, cyber services, etc.

In general, accessing the Internet and email accounts or bank accounts, in particular brokerage accounts, currently requires the user to learn and memorize a number of steps, which is especially difficult for persons who do not have computers of their own and/or who may be unfamiliar with using the Internet. This is often the case for customers of cyber cafés or cyber boutiques, as well as for the generation that has not grown up using the Internet.

The various steps are as follows:

- the need for relatively complex parameterization of the remote connection. In the case of using prepaid access cards, this requirement may have to be carried out repeatedly (with each new card).
- the need to search for and launch the remote connection of the workstation on the Internet.
- The need to search for and launch an Internet browser.

[1] Numbers in the margin indicate pagination in the foreign text.

- The need to create one's own email account, and therefore most often needing the assistance of another person or to risk making errors on one's own.
- The need to enter a URL address for accessing a server each time one checks one's email account, bank account, or brokerage account.
- The need to enter a login, possibly in the presence of others (contexts of public places, cyber boutiques, etc.) with a risk of identification by others at each query.
- The need to memorize the 7 previous steps and all personal access information.
- The difficulty of knowing the exact connection time on a public machine. Even though service is sold on the basis of duration, "cyber café"-type services are generally not equipped with counting systems.
- Major risks of nonconfidentiality for queries made on a public machine (cyber café type).

These risks are generated by three factors:

1. The keyboard inputting of access codes may be observed by a third party with negative intent. This inputting may also be the object of remote electromagnetic spying, recording the keystrokes made and the electromagnetic emissions from the screen.
2. Some especially skillful pirates are able to perform temporary installations of false sites in proxy mode. This type of site, whose apparent address is that of the pirated site, will capture, for several days, all of the traffic to the pirated site. They need

only memorize the logins and passwords of connecting users, redirect the request towards the real site, then later fraudulently use the logins and passwords stolen during the operation. This type of piracy is nearly impossible to detect.

/2

3. The files consulted over the Internet, including pages with access code entries, ordinarily remain in the form of temp files and page histories, easily accessed after the departure of the user, by any person having basic knowledge of this Internet feature. The persistence of such information on the used machine may cause great harm to the user when a non-legitimate person is able to discover the contents, nature, or even query addresses of the legitimate holder.

Only a small part of these disadvantages is prevented, as of this writing, by methods using chip cards. However, such methods involve the serious disadvantage of requiring a special reader that is extremely hard to find on the current microcomputer market. Another disadvantage of chip cards is linked to their limited storage capacity; 64 kilo-octets at most, which does not enable easy use of major software operations.

The method of the invention relates to an automated mode for access and/or for connection and secure entry to the Internet, involving:

- an access device, including a software program in CD form (or recorded on a diskette) with a capacity exceeding 250 kilo-octets, with the medium being selected so as to be compatible with the greatest possible number of current

nonspecific and nondedicated computers, specifically of the PC type, that do not have nonstandard equipment. Therefore, the present invention excludes the use of media of the chip card type, for the abovementioned reasons. The method of the invention enables access to free email accounts (Webmail), to bank or brokerage accounts, or to Internet Access Provider sites, by the greatest number of individuals, including and in particular by persons who do not own their own equipment and do not have a background in computers.

- A device for erasing temporary operations memorized on the machine used. This device ensures query confidentiality: no trace of the user remains on the machine if the user wishes.
- A device for generating specific access codes for each of the CDs used, using an automatic random process to which is added an automatic pseudorandom process and a decision-making process of the operator generating the codes.
- A device for integrating the generated codes into each specific file of the CDs.
- A device for compressing the files for each CD, containing the codes generated as described above.
- A device for rereading burned CDs to be sent to a distributor client so that he may himself identify the integrated access codes to be supplied to the final user; these codes are not known by the manufacturing teams.
- A device for displaying commercial or informational communications.

Features of the Access Device /3

The access device, integrated into a core software program burned onto the CD, meets the following requirements:

- Launching of the process in Autorun mode (using Windows) from the CD.
- Possibility of automatic parameterization of a remote connection by subscription or by prepaid card, via simplified entry (login and password only, without manipulations, verifications, or searches).
- Entry of a confidential code with 4 to 5 characters, depending upon the version, authorizing opening of the session.
- Automatic launching of the Internet browser without search or selection.
- Automatic launching of the connection request.
- Automatic launching of an Internet page including the display of a strip of buttons and command menus, as well as the page or pages of commercial or informational communication from one or several partners in cyclical rotation over time.
- Direct launch via selection on a button (mailbox) or on a menu of one or several preconfigured mailboxes and of one or several bank accounts.

* Autorun Mode:

In the current state of the art of automatic launching of software applications, current CD readers offer, using Windows, an Autorun function that makes it possible to launch automatically, upon insertion of the CD, conventional software applications of the

executable type (the file name ending for files of these applications is either .com, .exe, or .reg) but that does not make it possible to open Internet-type files ending in .htm, .html, .asp, or .php.

The access device according to the method of the invention enables this operation via an internal software programming method. The Autorun function calls an executable file that manages various functions, including erasing functionalities. This executable file makes it possible to call Internet-type files. It then becomes possible to obtain automatic display of one or several .htm or .html pages.

* Parameterization of a remote connection.

The access device of the method of the invention enables parameterization of a remote connection starting from the usual components of a prepaid Internet card or from the parameters of an Internet subscription account, by simply entering the login and the password of the prepaid card or of the account.

The access device of the method of the invention performs the necessary writing into the Windows registry so that a properly-parameterized remote connection is constituted. In particular, it performs a parameterization that takes into account a possible output code towards the RTC network. Additionally, the device verifies that the launch of the connection request is properly parameterized to automatically display each time an .htm or .html file is opened.

/4

When a prepaid-type card is used, variations may be planned for.

* Protection by confidential code.

The access protection device at a session of the method of the invention (entry of a 4- or 5-character confidential code) is innovative in that the entry of the code authorizes the opening of a session that in turn leads to the software emission of one or several long identifying codes, which are of course different from the 4- or 5-character code, without needing to use a chip card. The entry of the short code, if it were to be the object of a fraudulent identification, could only be used by gaining possession of the CD to which it is specifically attached.

Hence, security is provided, in innovative fashion, on two levels: first, it is necessary to have the CD, as well as a 4- or 5-character code, in order to validate the opening and thereafter to cause access via stealth generation and software sending of addresses and passwords. The passwords, the addresses, and the 4- or 5-character code are all different.

Important note:

The device for integrating keys into the specific file(s) of a CD and the device for compressing file(s) that have keys could be designed so that the keys appear "uncoded" in the files present on the CD. However, this practice would not ensure that the keys have the value of a unique signature to the extent that any computer file may be copied. Copying and ill-intentioned use of the keys would then be possible.

The device for integrating the keys into the specific file(s) of a CD and the compressing device are therefore the object of complex coding intended exclusively for ensuring the uniqueness and validity of the sending of a key, by making unintelligible the files present on the CD, so as to provide to the CD owner a means for sufficient security in identifying himself to authorized third parties. The key, when used, is generated stealthily, then sent in unintelligible characters. It therefore circulates uncoded over the Internet network. In no case may these devices enable transmission of unintelligible information. So this is not encrypting of information, but rather a mode for securing identification by making it impossible to be reproduced.

* Other complementary services.

The access device of the method of the invention also offers various options, in a menu, such as applications or tools enabling access to specific telephony or visiophony Internet sites. Indeed, a certain number of interesting sites require the user to download onto the machine he is using. The problem becomes burdensome when a single user uses several different machines, such as in cyber cafés. He must perform long downloads often for a single service. Making these applications available on the CD makes these downloads unnecessary.

Features of the erasing device.

The erasing device of the method of the invention is integrated into the core software. /5

Once the query is stopped, it asks all open Windows to be closed.

It then proceeds, via default, to erase all temp files, cookies, recent files, various histories, and resets the bands corresponding to the files erased from the hard drive, and finally does another erasing. If desired, the user may limit erasures of a given category of his choice, with the default option being full erasure.

Additionally, in case an access to a remote connection is created via prepaid card or via subscription, the erasure of this connection is automatic in order to prevent another user to be able, once the machine is available, to use the account opened by his predecessor.

Features of the code generation device.

* Preconfiguration of the mailbox:

If we wish to prevent a large number of users from having to create their mailboxes, it is necessary to provide said mailboxes, already created a priori. Creating large numbers of mailboxes in advance presents two technical problems connected to the possible disclosure of these mailboxes' existence to unauthorized third parties.

1. Impossibility of performing a sequential address creation.

Let's assume that we are creating a series of mailboxes, numbered from 0 to 1,000,000 for example; it would be easy for an unscrupulous individual, once he had learned of the existence of such a sequence, to systematically exploit the constituted

database in order to send vast numbers of advertising messages. The users of said mailboxes would then be inundated with unsolicited messages (spam).

2. To the extent that the address of a user is disclosed (normal situation), the password of this mailbox must not respond to a sequential composition mode. Indeed, a "pirate" wishing to consult the mailbox of a user by hacking into it would only have to interrogate systematically series of sequential alphanumerical words. The code generating device of the method of the invention makes it possible to obtain addresses and passwords that get around the abovementioned difficulties.

* Address of the mailbox.

A specific feature of the device of the invention generates pseudorandomly the mailbox addresses to be created in great numbers:

The generation of electronic mailboxes of the method of the invention is carried out so that the first character can only be one of 15 letters of the alphabet and 2 of the numerals from 0 to 9. For the following characters, the used series will, of course, be different.

Hence, even if we have to generate several tens of millions of different names, the use of 8-character names is sufficient for creating "holes" in the explorable series that are so large that they would have the effect of inundating with error messages any individual trying to send messages on sequential names, which would have only 1 chance in 40,000 of reaching an active mailbox. The generator may be constructive mechanographically or via software, and programmed in any adapted language. The generation of names,

generally meaningless ones, composed of alphanumerical characters, may be random or sequential. /6

* Password.

In order to prevent knowledge of several codes from making it possible to reconstitute valid code series, the password(s) of the mailbox or the identification words for access to bank accounts are generated in dual fashion: automatic random generation and decisional random generation.

For a code of 9 alphanumerical characters for example, one way of proceeding consists of successively generating 3 columns of 5000 3-character codes, then of placing the columns side by side according to an order decided upon by the operator. An operation of concatenating the 3-character groups will yield 9-character codes within which it will be extremely difficult, even impossible, to find a compositional mathematical law for reconstructing unknown codes. This method prevents the reconstitution of code series based on the knowledge, acquired by accident or on purpose, of an existing and valid series of codes.

The password for an electronic mailbox or for accessing a bank account according to the invention is created by alphanumerical words from 9 to n characters, according to the developed applications. When used to open electronic mailboxes, the password can only have 9 characters, whereas in financial applications for opening query pages or pages listing bank transactions, the password may have many more characters. Any other

device enabling random generation of words whose length is sufficient to guarantee enough security could be implemented in the method of the invention.

In order to protect the access mode from possible pirating of passwords using copies of proxy sites, sending of the password towards the targeted site's homepage occurs via a dialogue mode established with the targeted page. The dialogue process is based on having the targeted site send a session identifier including a part dated to the nearest second and a part giving a composition order of several sections of the long password. The access device of the method of the invention then composes the long password to be sent by concatenating a set of sections of the long password extracted from the coded compressed file stored on the disk. This concatenation is performed according to the organization requested by the session identifier received from the targeted site. The targeted site's homepage then proceeds to recompose the long password, then compares it to the database of valid long passwords, then opens access if the forwarded word is valid.

This transmission mode makes it possible to block pirating via fake proxy servers, to the extent that the transmitted long password is different at each request. The fact that one has a given version of one emission does not mean that the targeted access may be opened at a later date.

Features of the generated code integration device.

The code integration device of the method of the invention cuts up and disperses sections of code inside a file composed of a series of about 20,000 meaningless but intelligible characters that are randomly generated, then cut up.

Features of the compression device.

The compression device of the method of the invention renders unintelligible the characters in the file and reduces its size to roughly 8000 characters.

/7

Features of the rereading device.

For obvious security reasons, the disks are "blind"-burned: the burning team never knows the disk access codes, nor does it know the long passwords.

To enable the distributor (generally a bank) to give its client the confidential code of the CD that he has received, the method of the invention includes a CD rereading device, existing in two variations: Variation 1: only enables reading of the CD's confidential code and its startup date (which triggers the need for the code). Variation 2: makes it possible, at full privilege, administrator-type level, to read all of the CD's codes, in case a questionable disk is physically returned.

Features of the communication display device.

In the current state of the art for Internet site display, no method exists that makes it possible to vary, by hourly or daily time slot, various sites displayed in full-page view based on a single command or a single address. The full-page display device of the method of the invention makes it possible to modify by time slots, even daily ones, the rotation of the display of Internet welcome pages of partner sites, regardless of whether they are for commercial, educational, informative, associative, charitable, or other purposes.

Features of the CD personal access security system.

In order to prevent an unauthorized person from using the CD without the knowledge of its legitimate owner, the startup of the process is linked to the entry of a 5-character case-sensitive personal code, involving nearly a billion possible combinations.

Three successive erroneous keyboard entries by the user cause the process to disconnect.

Additionally, if the user reiterates manually or via software a certain number of tens of tries to enter unknown codes, the process goes into a permanent loop and it is then necessary to shut down the machine and reboot it.

Lastly, this code is not active throughout the entire manufacturing process, such that the burning teams can test the base functionalities of the CD using a generic alternative code. Up to this date, however, the specific functionalities (mailbox and account access) are not accessible.

This feature makes it necessary for the product distributor (banks in particular) to be able to recognize which code corresponds to a specific disk prior to attribution to each client; this need is met by the rereading device cited above.

The method of the present invention therefore has the role, while preserving and reinforcing all of the usual confidentiality criteria, of:

- innovatively enabling highly-simplified parameterization, requiring no specific background, of the remote Internet connection, specifically starting from prepaid cards or subscription notifications that have only a login and a password.

/8

- enabling automatic erasure of the remote connection and its credit following use on a machine used by other persons. This step is innovative in that such an erasure is ordinarily only possible by successively opening up various Windows intervention steps.
- Innovatively enabling automated and secured access to one or several Internet sites that ordinarily require keyboard inputting of URLs, logins, and passwords.
- Eliminating the need to have the user create an electronic mailbox.
- Reducing to a minimum the risk of sending serial unsolicited messages.
- Reducing to a minimum the risks of having the created mailboxes or targeted bank accounts undergo hacking.
- Innovatively eliminating the need to launch an Internet browser.

- Eliminating the need to enter an access URL for each query.
- Innovatively eliminating the need to type in a login for each query.
- Innovatively eliminating the need to memorize personal access information.
- Innovatively eliminating the risk of direct surveillance or remote electromagnetic spying of access to the electronic mailbox or to bank or brokerage accounts.
- Eliminating the risk of consulting codes after using a public site by erasing temp files created during use, along with any traces thereof.
- Eliminate uncertainty concerning duration of connection to the Internet.
- Prevent consultation of email dedicated to the device according to the method by unauthorized third parties.

The method of the invention also authorizes the user to gain direct access to a selection of various services of interest to any mobile person: international phone books, email address searches, "cyber café"-type Internet service searches, on-line translation, currency conversion, travel reservations, etc.

The method of the invention also uses a time counter device making it possible to know how long the connection has lasted so that the time used by the user may be fairly evaluated. This counter may be a mechanical or electromagnetic device that is triggered upon inserting the recording medium into the reader, or it may be a software program.

In a variation named SW@Pmail, the method of the invention relies on a specific Internet site (http://www.keesay.com) used for managing the various series to which the

method provides access, as well as on records of individual applications burned on CD-ROMs in business card format, which can be read by any current drawer-style CD reader.

- The Internet site http://www.keesay.com enables a manager to direct the various operations needed for proper operation of the communication display method.

/9

The electronic mailbox for each SWAPmail is generated on a Webmail-type server, such as Nameplanet.com for example, enabling access from any station connected to the Internet.

- The various software programs and applications that constitute the individualized part of the SWAPmail method are burned onto a CD in business card format.

Automatic launching occurs by calling upon the Autorun function of current CD readers. The launching of this application then leads, via adequate programming, to the launch of Internet-type files (.htm or .html extensions) integrating the addresses and access passwords to the various corresponding preconfigured personalized sites (electronic mailbox, bank accounts). The launch of the SWAPmail.htm Internet-type file leads to the availability of the direct opening function of the electronic mailbox, without the name or the full password for the mailbox being typed in or appearing on the screen.

The user may then launch opening of the mailbox by clicking on the "Mail" button (of course, the name of the button changes depending upon the language in which SWAPmail is created), or any button corresponding to a preconfigured bank account.

The various .htm files cited above are stealthily generated in memory. That is, their existence in memory in intelligible code does not exceed the duration necessary for sending requests to the relevant servers. These files disappear as soon as they have been used.

Opening of the electronic mailbox then occurs, in innovative fashion, without having the name or password of the mailbox typed in or being fully displayed on the screen. The launch, starting from the initial core software program, of other Internet-type files (.htm or .html extensions) may lead, if the version of the application is so designed, to the direct opening of query pages for bank accounts, by sending alphanumerical passwords of appropriate length and at the desired security level to the relevant sites.

The first way to display communication pages that are differentiated in time is to program, directly into the SWAPmail CD's batch file or into the display file to which it enables access, a sequence enabling access to various site addresses, according to cyclical and predetermined time periods.

- another way to obtain a differentiated display consists of cyclically changing the content of the address or addresses to which the CD file enabling the display is pointing.

Variations on the preceding version may also be designed:

One of the variations on the application of the method of the invention relates to making a CD that integrates all or part of the devices of the method of the invention,

making it possible to open several email mailboxes instead of only one, as described above.

Another variation on the application of the method relates to making a CD that integrates all or part of the devices of the method of the invention, making it possible to open several bank, brokerage, or insurance-type service management accounts instead of only one, as described above.

Another variation on the application of the method may relate to making a CD that integrates all or part of the devices of the method of the invention, enabling automated access to the Internet via login and password codes of the "prepaid card" type, using a single-use (non-rechargeable) code, including the creation of access to the remote connection and its erasure at the end of the session. /10

Another variation on the application of the method may relate to making a CD that integrates all or part of the devices of the method of the invention, enabling automated access to the Internet via login and password codes of the "prepaid card" type, using a repeated-use (rechargeable by code coupon) code, including the creation of access to the remote connection and its erasure at the end of the session.

The method of the invention is appropriate for industrial manufacture in various countries, aims to offer facilitated and secure access to public Internet access sites for a very large number of users worldwide who are neophytes on the Internet, as well as an economical and uncomplicated way to use it via prepaid card. The method of the

invention would help develop a kind of international *poste restante* that is accessible by the user from any point in the world that is connected to the Internet. The method of the invention may also make it possible to greatly develop bank queries and transactions over the Internet thanks to its ability to protect performed transactions.

Moreover, regarding secure payment over the Internet, the method of the invention makes it possible to validly replace the use of a bank card as a means of identification, with a higher level of security than any attained to date. Indeed, it should be noted that the bank card is the weak link in the chain of Internet payments, which is not the case for the method of the invention. /11

CLAIMS

1. Method for automated Internet access via a computer program characterized in that it involves the following steps:

a) Following insertion of a medium into a PC reader, the automatic launch from the computer program, present on the CD, (Autorun) of a validation prompt, leading to validation by typing of a short, easily-memorized code for accessing use of programs stored on the medium;

b) The display by the abovementioned computer program of a prompt to select an Internet access connection already on the machine or to automatically create a new connection;

c) The launch of an Internet-type file (.htm or .html) directly from the medium;

d) The display, by the abovementioned computer program, of a determined Internet environment, including at least one electronic mailbox and various personalized services or accounts, where access to the mailboxes and to these various services occurs via a direct link, without typing in codes via stealthy software transmission of addresses and passwords, unlike the short code mentioned in b), without requiring entry of said passwords and addresses, and including a set addressing towards a site or sites offering the possibility of modifying over time the content of the Internet sites accessed at startup;

e) At the end of the session, erasure by the computer program of any traces on the machine used, involving either an erasure of Internet temp files created during the session, query histories, summaries of recently-used files, and more generally any and all traces of how the machine was used.

2. Removable medium supporting the method of Claim 1, such as a CD or diskette, characterized in that it does not require the use of unusual equipment specifically used for reading said medium, as might be necessary for chip cards.

3. Method according to Claim 1, characterized by the optional parameterization of Internet access using prepaid cards that have specific codes on each card, comparable to so-called "non-technical" coded telephone cards, as a replacement for resident access.

4. Method according to Claim 3, characterized by the optional erasure, at the end of each use, of the previously-parameterized remote Internet connection.

5. Method according to Claim 1, characterized by:

a) The optional integration into the medium of Claim 2 of an average identifier by creating random or pseudorandom names, using partial generations of sections of alphanumerical passwords by algorithm, followed by concatenation via mixing the sections based on human decision;

b) The optional integration into the medium of Claim 2 of a strong identifier, such as an encrypted file or encryption mode for the internal identifier of the medium.

6. Application of the method of Claim 1 for querying and/or management of on-line bank accounts via the Internet. /12

7. Application of the methods in claims 1 and 3, for paid access using prepaid cards at sites protected by personalized account codes.

8. Computer-produced program including programming code instructions recorded on a medium that is usable in a computer in order to perform the steps listed in claims 1, 3, 4, and 5.

2822255

FRENCH REPUBLIC
INPI
NATIONAL INDUSTRIAL PROPERTY INSTITUTE

PRELIMINARY SEARCH REPORT

National Registration No.: FA 612727
FR 0101855

Established on the basis of the most recent claims filed prior to initiating the search

PERTINENT DOCUMENTS			
Category	Document citation with indication, if necessary, of pertinent sections	Claim involved	Category attributed to the invention by INPI
A	GB 2,346,239 A (IBM) August 2, 2000 (08-02-2000) * abstract * * page 3, line 14 – page 4, line 2 * * page 7, line 1 – page 8, line 2 * * page 8, line 33 – page 9, line 19 * * page 10, line 23 – page 11, line 16 * * figures 3,4 *	1,6,8	G06F9/445
A	WO 00 49505 A (HENDRICK COLIN) August 24, 2000 (08-24-2000) * page 14, line 17 – page 15, line 15 * * page 18, line 14 – line 25 *	1,6	
A	US 5,987,612 A (SHIRAISHI YOSHIHIKO ET AL) November 16, 1999 (11-16-1999) * abstract * * column 1, line 61 – column 2, line 30 * * column 7, line 25 – line 42 * * column 8, line 8 – line 42 * * column 9, line 9 – line 16 *	1,3,7	
A	US 5,960,085 A (DE LA HUERGA CARLOS) September 28, 1999 (09-28-1999) * column 5, line 12 – line 27 *	1,4	

			Technical fields searched (Int.Cl.7)
A,P	WO 00 62249 A (STOCK ROBIN; GMS SOFTMED SC (BE)) October 19, 2000 (10-19-2000) * page 1, line 1 – line 30 * * page 2, line 28 – line 34 * * page 4, line 25 – line 35 * * page 8, line 23 – line 34 * * Claim 12 *	1,2,6,8	G06F G07F H04L

	Date search completed: April 29, 2002	Examiner: Arbutina, L.

CATEGORY OF THE CITED DOCUMENTS	
X: Especially pertinent on its own Y: Especially pertinent in combination with another document in the same category A: Technological background O: Unwritten disclosure P: Intermediate document	T: Theory or principle on which the invention is based E: Prior patent document, but published on the filing date or after this date D: Cited in the application L: Cited for other reasons A: Member of the same family, corresponding document

2822255

ENCLOSURE TO PRELIMINARY SEARCH REPORT

FOR FRENCH PATENT APPLICATION NO. FR 0101855 FA 612727

This enclosure lists members of the family of patents relating to the patent documents cited in the abovementioned preliminary search report.
Said members are found in the computer files for the European Patent Office dated 04-29-2002.
The information provided is given for informational purposes and in no way engages the liability of the European Patent Office or of the French Administration.

Patent document	Publication	Member(s) of family of	Publication date

cited in search report	date	patent(s)	
GB 2346239 A	08-02-2000	JP 2000222362 A	08-11-2000
WO 0049505 A	08-24-2000	AU 3002100 A WO 0049505 A1	09-04-2000 08-24-2000
US 5987612 A	11-16-1999	CN 1190301 A JP 1022446 A SG 65035 A1	08-12-1998 08-21-1998 05-25-1999
US 5960085 A	09-28-1999	US 6259654 B1 US 6032155 A	07-10-2001 02-29-2000
WO 0062249 A	10-19-2000	BE 1013244 A3 BE 1013531 A3 AU 3137600 A WO 0062249 A2	11-06-2001 03-05-2002 11-14-2000 10-19-2000

For any information regarding this enclosure: See Official Journal of the European Patent Office, No. 12/82.